guidelines, as necessary, to ensure consistency with NISP policies and procedures. Such reviews should normally occur during routine oversight visits, when there is indication of a problem that comes to the attention of the Director, ISOO, or after a change in national policy that impacts such regulations, rules, or guidelines. The Director, ISOO, shall provide findings from such reviews to the responsible department or agency.

§ 2004.12 Reviews by ISOO [102(b)(4)].

The Director, ISOO, shall fulfill his monitoring role based, in part, on information received from NISP Policy Advisory Committee (NISPPAC) members, from on-site reviews that ISOO conducts under the authority of EO 12829, as amended, and from complaints and suggestions from persons within or outside the Government. Findings shall be reported to the responsible department or agency.

Subpart B—Operations

§ 2004.20 National Industrial Security Program Operating Manual (NISPOM) [201(a)].

(a) The NISPOM applies to release of classified information during all phases of the contracting process.

(b) As a general rule, procedures for safeguarding classified information by contractors and recommendations for changes shall be addressed through the NISPOM coordination process that shall be facilitated by the Executive Agent. The Executive Agent shall address NISPOM issues that surface from industry, Executive Branch departments and agencies, or the NISPPAC. When consensus cannot be achieved through the NISPOM coordination process, the issue shall be raised to the NSC for resolution.

§ 2004.21 Protection of Classified Information [201(e)].

Procedures for the safeguarding of classified information by contractors are promulgated in the NISPOM. DoD, as the Executive Agent, shall use standards applicable to agencies as the basis for the requirements, restrictions, and safeguards contained in the NISPOM; however, the NISPOM requirements may be designed to accommodate as necessary the unique circumstances of industry. Any issue pertaining to deviation of industry requirements in the NISPOM from the standards applicable to agencies shall be addressed through the NISPOM coordination process.

§ 2004.22 Operational Responsibilities [202(a)].

(a) *Designation of Cognizant Security Authority (CSA).* The CSA for a contractor shall be determined by the preponderance of classified contract activity per agreement by the CSAs. The responsible CSA shall conduct oversight inspections of contractor security programs and provide other support services to contractors as necessary to ensure compliance with the NISPOM and that contractors are protecting classified information as required. DoD, as Executive Agent, shall serve as the CSA for all Executive Branch departments and agencies that are not a designated CSA. As such, DoD shall:

(1) Provide training to industry to ensure that industry understands the responsibilities associated with protecting classified information.

(2) Validate the need for contractor access to classified information, shall establish a system to request personnel security investigations for contractor personnel, and shall ensure adequate funding for investigations of those contractors under Department of Defense cognizance.

(3) Maintain a system of eligibility and access determinations of contractor personnel.

(b) *General Responsibilities.* Executive Branch departments and agencies that issue contracts requiring industry to have access to classified information and are not a designated CSA shall:

(1) Include the Security Requirements clause, 52.204–2, from the FAR in such contracts;

(2) Incorporate a Contract Security Classification Specification (DD 254) into the contracts in accordance with the FAR subpart 4.4;

(3) Sign agreements with the Department of Defense as the Executive Agent for industrial security services; and,